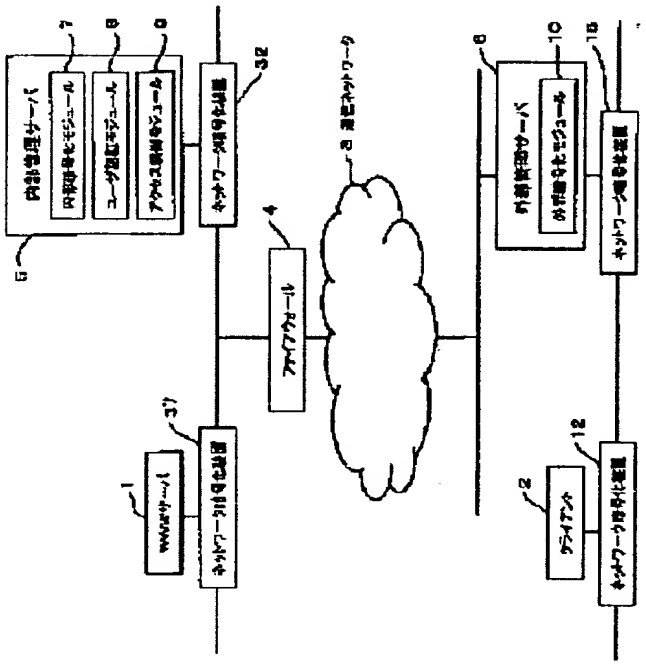
METHOD FOR SAFE INFORMATION TRANSMITTING/SHARING SERVICE

Publication number: JP2000112860
Publication date: 2000-04-21
Inventor: HARADA MASAFUMI
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
- international: ***G06F13/00; H04L9/08; H04L9/32; H04L29/08;*** **G06F13/00; H04L9/08; H04L9/32; H04L29/08;** (IPC1-7): G06F13/00; H04L9/08; H04L9/32; H04L29/08
- European:
Application number: JP19980280266 19981001
Priority number(s): JP19980280266 19981001

Abstract of **JP2000112860**

PROBLEM TO BE SOLVED: To provide a safe information transmitting/sharing service convenient for users. SOLUTION: In a network system consisting of a WWW server 1 for transmitting information an inside management server 5 for safely managing information transmitting/sharing service, a fire wall 4, a communication network 3, a client 2 requesting information service, and an outside management server 6 for safely managing the information transmitting/sharing service, a service request from the client 2 is enciphered by the server 6 and sent to the server 5 through the network 3. The server 5 executes deciphering, user certification and access control for the sent request and sends the processed request to the server 1. The server 5 enciphers a service response from the server 1 and sends the enciphered response to the server 6 through the network 3 and the server 6 deciphers the enciphered response and sends the deciphered response to the client 2.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－112860
（P2000－112860A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５４	Ｃ０６Ｆ　13/00	３５４Ｚ	５Ｂ０８９
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｅ	５Ｋ０１３
9/32			６０１Ｃ	５Ｋ０３４
29/08			６７１	
		13/00	３０７Ｚ	

審査請求　未請求　請求項の数８　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－280266

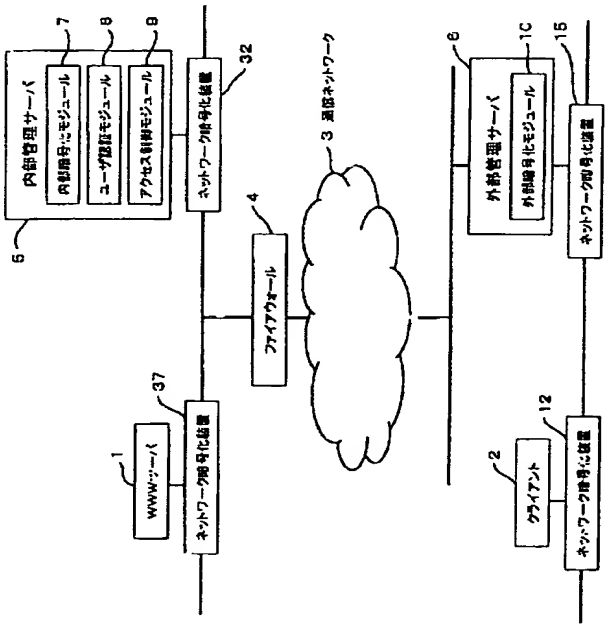
(22)出願日　平成10年10月１日(1998.10.1)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　原田　雅史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5B089 AA21 AA22 AB01 AC05 AE05 CE03 DD07
5K013 AA00 AA03 BA03 GA01 GA08
5K034 AA17 EE10 HH01 HH02 HH06

(54)【発明の名称】　安全な情報発信・共有サービス方法

(57)【要約】
【課題】　利用者の利便性の良い、安全な情報発信・共有サービスを提供する。
【解決手段】　情報を発信するＷＷＷサーバ１と、情報発信・共有サービスの安全管理をする内部管理サーバ５と、ファイアウォール４と、通信ネットワーク３と、情報サービスを要求するクライアント２と、情報発信・共有サービスの安全管理をする外部管理サーバ６とからなるネットワークシステムにおいて、クライアント２からのサービス要求は、外部管理サーバ６において暗号化され、通信ネットワーク３を介して内部管理サーバ５へ送られ、復号、ユーザ認証、及びアクセス制御がされ、ＷＷＷサーバ１へ送られる。ＷＷＷサーバ１からのサービス応答が、前記内部管理サーバ５において暗号化され、通信ネットワーク３を介して前記外部管理サーバ６へ送られ、復号され、クライアント２に送られる。



【特許請求の範囲】
【請求項１】　外部からの不正アクセスを防止するための不正アクセス防止手段によって内部と外部に分割されたネットワークにおいて、
内部ネットワークは、内部ネットワーク上からクライアントの前記情報発信・共有サービス要求に応じて情報を発信するWWWサーバと、
前記クライアントと前記WWWサーバ間の通信内容を暗号化・復号化する内部暗号化モジュールと、クライアントのユーザ認証を行うユーザ認証モジュールと、クライアントのアクセス制御を行うアクセス制御モジュールとを備え、内部ネットワークにおいて情報発信・共有サービスの安全管理をする内部管理サーバとを有し、
前記外部ネットワークは、ローカルネットワークと通信ネットワークからなり、前記外部ローカルネットワークは、外部ローカルネットワーク上から情報発信・共有サービスを要求するクライアントと、
クライアントとWWWサーバ間の通信内容を暗号化・復号化する外部暗号化モジュールを備えた情報発信・共有サービスの安全管理をする外部管理サーバとを有し、
クライアントからの情報発信サービス要求は、前記外部管理サーバにおいて暗号化され、通信ネットワークを介して前記内部管理サーバへ送られ、
前記内部管理サーバにおいて、復号、ユーザ認証、及びアクセス制御がされた後に、前記WWWサーバへ送られ、
前記要求に対する前記WWWサーバからの情報発信サービス応答が、前記内部管理サーバにおいて暗号化され、通信ネットワークを介して前記外部管理サーバへ送られ、
前記外部管理サーバにおいて、復号されて、前記クライアントに送られることにより、クライアントが情報発信・共有サービスを受けることを特徴とする情報発信・共有サービス方法。
【請求項２】　前記クライアントと前記WWWサーバ間の情報発信・共有サービスをＨＴＴＰにて行うことを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項３】　前記クライアントのユーザ認証は公開鍵と秘密鍵を使用した電子証明書を用いて行うことを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項４】　前記内部管理サーバ及び外部管理サーバは、クライアントとWWWサーバ間の情報データを一時的に記憶するキャッシュを有し、
各管理サーバは、要求に対する応答が各管理サーバ上のキャッシュにある場合は、その応答を取り出してクライアントに送ることを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項５】　前記外部管理サーバは前記クライアント上のキャッシュの情報を消去するクライアントキャッシュ消去手段を有し、
クライアントの利用者が交代する毎に、クライアントキャッシュの情報を消去することを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項６】　前記WWWサーバ上に暗号化・復号化手段を有し、WWWサーバと前記内部管理サーバとの間の通信データについても暗号化することを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項７】　前記クライアント上に暗号化・復号化手段を有し、前記クライアントと前記外部管理サーバとの間の通信データについても暗号化することを特徴とする請求項１記載の情報発信・共有サービス方法。
【請求項８】　前記内部管理サーバと前記外部管理サーバ間における暗号化通信において、暗号化に用いる暗号鍵の交換時期を変化させることを特徴とする請求項１記載の情報発信・共有サービス方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、内部ネットワークと外部ネットワーク相互間における暗号化通信を基本とした安全な情報発信・共有サービス方法に関するものである。
【０００２】
【従来の技術】情報通信技術の発達、特にインターネットの国際的な普及に伴い、情報の入手が容易になった反面で、第三者による不正侵入や情報の漏洩が問題となっており、安全に情報提供サービスができるネットワークシステムが必要とされている。
【０００３】図１に、“三菱セキュアＷｅｂアクセスＭｉｓｔｙＧｕａｒｄ＜ＴＲＵＳＴＷＥＢ＞”による従来の情報発信・共有システムの概要を示す。
【０００４】情報発信・共有サービスを要求するクライアント８２が、通信ネットワーク８３と接続され、この通信ネットワーク８３が、ファイアウォール８４を介して、内部ネットワークと接続されている。内部ネットワークはファイアウォールにより、外部からの不正アクセスから保護されているネットワークである。一方外部ネットワークは、内部ネットワーク以外のネットワークである。
【０００５】内部ネットワーク上に、情報発信・共有サービスを提供するWWWサーバ８１と、情報発信・共有サービスのアクセス制御を行うアクセス制御サーバ８５が設けられている。アクセス制御サーバ８５は、暗号処理を行う内部暗号モジュール８７と、アクセス制御を行うアクセス制御モジュール８８と、アクセス制御を行う際に参照するユーザ毎の情報を管理するアクセス制御リスト９０で構成されている。クライアント８２は、暗号処理を行うクライアント側暗号モジュール８６と、アクセス制御サーバ用暗号鍵を管理するアクセス制御サーバリスト８９で構成されている。ここで、各サーバ及びクライアントは、情報処理装置であり、各モジュール及び

アクセス制御リストはソフトウエアである。

【０００６】続いて従来の情報発信・共有サービスにおける情報の要求及び提供方法について説明する。

【０００７】クライアント８２が情報発信・共有サービス要求（以下サービス要求という）を作成すると、クライアント側暗号モジュール８６がサービス要求を解析し、アクセス制御サーバリスト８９を参照し、以下の処理により暗号化する。

【０００８】１）一時暗号鍵を生成する。２）アクセス制御サーバリスト８９からアクセス制御サーバ８５用の公開鍵を取り出す。３）サービス要求を１）で生成した一時暗号鍵で暗号化する。４）この一時暗号鍵を２）で取り出したアクセス制御サーバ８５用の公開鍵で暗号化する。５）アクセス制御サーバリスト８９からアクセス制御サーバ８５のアドレスを取り出す。６）サービス要求のアドレスをWWWサーバ８１からアクセス制御サーバ８５へ変更する。

【０００９】こうして暗号化されたサービス要求及び一時暗号鍵が情報ネットワーク内部ネットワークのアクセス制御サーバ８５へ送られる。アクセス制御サーバ８５では以下の処理により暗号化されたサービス要求を復号する。１）アクセス制御リスト９０からアクセス制御サーバ８５用の秘密鍵を取り出す。２）送られてきた一時暗号鍵を取り出したアクセス制御サーバ８５用の秘密鍵で復号する。３）復号された一時暗号鍵を用いて暗号化されたサービス要求を復号する。

【００１０】復号されたサービス要求に対してアクセス制御モジュール８８がアクセス制御リスト９０を参照してアクセス制御を行う。すなわちWWWサーバ８１へのアクセス可否の判断を行う。WWWサーバ８１へのアクセスが許可された場合はサービス要求がWWWサーバ８１へ送られる。一方アクセスが許可されない場合はエラーメッセージがクライアント８２へ送られ、手続きは終了する。

【００１１】サービス要求を受け取ったWWWサーバ８１はサービス要求に対するサービス応答をアクセス制御サーバ８５に送り返す。アクセス制御サーバ８５は以下の処理を行いサービス応答を暗号化する。１）アクセス制御サーバリスト８９からクライアント８２用の公開鍵を取り出す。２）サービス応答を一時暗号鍵を用いて暗号化する。３）一時暗号鍵をアクセス制御リスト９０から取り出したクライアント８２用の公開鍵で暗号化する。４）ネットワーク８３上に存在する各種サーバ上でのキャッシュを禁止する命令を追加する。

【００１２】暗号化され、キャッシュ禁止命令が追加されたサービス応答及び一時暗号鍵がアクセス制御サーバ８５からクライアント８２へ送られる。クライアント８２では以下の処理を行い暗号化されたサービス応答を復号化する。１）アクセス制御サーバリスト８９からクライアント８２用の秘密鍵を取り出す。２）送られてきた一時暗号鍵をクライアント８２用の秘密鍵で復号する。３）復号された一時暗号鍵を用いて暗号化されたサービス応答を復号する。

【００１３】このようにクライアント８２とWWWサーバ８１間で情報を暗号化して通信することにより、第三者に知られることなく安全な通信が可能となる。また、外部からの内部ネットワークへの不正なアクセス侵入や内部データの漏洩は、ファイアウォール８４によっても防止される。また、アクセス制御サーバにおけるアクセス制御を行うことにより、情報を利用できる利用者を限定できる。

【００１４】

【発明が解決しようとする課題】しかし、従来の情報発信・共有システムでは、利用者が情報発信・共有サービスを受けるためには、各クライアント８２が、クライアント側暗号モジュール８６及びアクセス制御サーバリスト８９のソフトウエアをインストールする必要があり、各クライアント利用者の負担となっていた。特に、多くのクライアントを有する社内ネットワークの管理者等は、各クライアント毎にクライアント側暗号モジュール８６等をインストールする必要があるため経済的負担が大きかった。またこのクライアント側暗号モジュール８６はセキュリティ製品であるためWWWサーバ８１上から利用者のクライアント８２にダウンロードすることは禁止されており、利用者は直接ソフトウエアを購入してインストールしなければならず、不便であった。

【００１５】さらに、マルチプラットホームの環境では、暗号モジュール開発者は、利用者のクライアントの種類に応じて、ＵＮＩＸ用、Ｍａｃｉｎｔｏｓｈ用、Ｗｉｎｄｏｗｓ３．１用等の様々な暗号モジュール８６をそれぞれ開発しなければならないという問題があった。

【００１６】さらに、情報の安全性確保の観点から通信ネットワーク８３上に存在する各サーバにキャッシュを残さないようにするため、キャッシュ禁止命令を追加して情報を送るが、このため、クライアントは、サービス要求毎に必ずアクセス制御サーバ８５経由でWWWサーバと通信しなければならず、トラフィックの混雑によるサービス要求に対する応答性能の劣化が問題となっていた。

【００１７】さらに、クライアント８２上におけるキャッシュの情報消去等の制御はクライアント８２上のみでしか行えないため、特に一台のクライアント８２を複数人が使用する場合にクライアント８２上のキャッシュから他人に情報が漏れるという問題点があった。

【００１８】さらに、ネットワーク内部のWWWサーバ８１とアクセス制御サーバ８５間は一般に平文で通信が行われているためこの間で盗難、改ざん等される可能性もあった。

【００１９】さらに、各アクセス制御サーバの性能は各装置によって差があるため、性能が低いアクセス制御サ

ーバであっても一定以上の応答性能を有することが要求されている。

【００２０】この発明は、上記のような問題点を解消するためになされたもので、ファイアウォール等で外部と内部に分割されたネットワーク上で安全な情報発信・共有サービスを提供することを目的とする。

【００２１】また、各クライアントがクライアント側暗号モジュール８６及びアクセス制御サーバリスト８９をインストールする負担を解消することを目的とする。

【００２２】また、ネットワーク８３上の各サーバにキャッシュを残せないことによる応答性能の劣化を改善することを目的とする。

【００２３】また、複数人が同一クライアント８２を使用する場合に生じるキャッシュからの情報漏洩を防止することを目的とする。

【００２４】また、内部ネットワーク上の通信データの盗聴、改ざんを防止することを目的とする。

【００２５】また、サービス要求に対する応答性能を向上させることを目的とする。

【００２６】

【課題を解決するための手段】この発明の請求項１に係る安全な情報発信・共有サービス方法は、外部からの不正アクセスを防止するための不正アクセス防止手段によって内部と外部に分割されたネットワークにおいて、前記外部のローカルネットワーク上で情報発信・共有サービスを要求するクライアントと、内部ネットワーク上からクライアントの前記情報発信・共有サービス要求に応じて情報を発信するWWWサーバと、内部ネットワーク上に設けられ、前記クライアントと前記WWWサーバ間の通信内容を暗号化・復号化する内部暗号化モジュールと、クライアントのユーザ認証を行うユーザ認証モジュールと、クライアントのアクセス制御を行うアクセス制御モジュールとを有し、内部ネットワークにおいて情報発信・共有サービスの安全管理をする内部管理サーバと、外部のローカルネットワーク上に設けられ、前記外部ネットワークは、ローカルネットワークと通信ネットワークからなり、前記外部ローカルネットワークは、外部ローカルネットワーク上から情報発信・共有サービスを要求するクライアントと、クライアントとWWWサーバ間の通信内容を暗号化・復号化する外部暗号化モジュールを有し、外部ローカルネットワークにおいて情報発信・共有サービスの安全管理をする外部管理サーバを備え、クライアントからの情報発信サービス要求は、前記外部管理サーバにおいて暗号化され、ネットワークを介して前記内部管理サーバへ送られ、前記内部管理サーバにおいて、復号、ユーザ認証、及びアクセス制御がされた後に、前記WWWサーバへ送られ、前記要求に対する前記WWWサーバからの情報発信サービス応答が、前記内部管理サーバにおいて暗号化され、通信ネットワークを介して前記外部管理サーバへ送られ、前記外部管理サーバにおいて、復号されて、前記クライアントに送られることにより、クライアントが情報発信・共有サービスを受けることを特徴とする。

【００２７】さらに、この発明の請求項２に係る安全な情報発信・共有サービス方法は、前記クライアントと前記WWWサーバ間の情報発信・共有サービスをＨＴＴＰにて行うことを特徴とする。

【００２８】さらに、この発明の請求項３に係る安全な情報発信・共有サービス方法は、前記ユーザ認証を公開鍵と秘密鍵を使用する電子証明書を用いて行うことを特徴とする。

【００２９】さらに、この発明の請求項４に係る安全な情報発信・共有サービス方法は、前記内部管理サーバ及び外部管理サーバは、クライアントとWWWサーバ間の情報データを一時的に記憶するキャッシュを有し、各管理サーバは、要求に対する応答が各サーバ上のキャッシュにある場合は、その応答を取り出してクライアントに送ることを特徴とする。

【００３０】さらに、この発明の請求項５に係る安全な情報発信・共有サービス方法は、前記外部管理サーバは前記クライアント上のキャッシュの情報を消去するクライアントキャッシュ消去手段を有し、クライアントの利用者が交代する毎に、クライアントキャッシュの情報を消去することを特徴とする。

【００３１】さらに、この発明の請求項６に係る安全な情報発信・共有サービス方法は、前記WWWサーバ上に暗号化・復号化手段を有し、WWWサーバと前記内部管理サーバとの間の通信データについても暗号化することを特徴とする。

【００３２】さらに、この発明の請求項７に係る安全な情報発信・共有サービス方法は、前記クライアント上に暗号化・復号化手段を有し、前記クライアントと前記外部管理サーバとの間の通信データについても暗号化することを特徴とする。

【００３３】さらに、この発明の請求項８に係る安全な情報発信・共有サービス方法は、前記内部管理サーバと前記外部管理サーバ間における暗号化通信において、暗号化に用いる暗号鍵の交換時期を変化させることを特徴とする。

【００３４】

【作用】クライアントからの情報発信・共有サービス要求は、外部管理サーバの外部暗号化モジュールにより暗号化される。ここで、暗号化方式としては、暗号化鍵と復号化鍵が同一の対称鍵暗号方式と、暗号化鍵から復号化鍵が容易に求められない公開鍵暗号方式があるがいずれを用いても良く、またその両方を用いてもよい。また、本発明は、クライアントではなく、外部の外部管理サーバに暗号化手段を有するため、より強固な暗号方式が開発された場合、内部管理サーバと外部管理サーバのモジュールを入れ替えるだけで新しい暗号方式に対応す

ることができる。

【００３５】暗号化された情報発信・共有サービス要求は、通信ネットワークを介して内部管理サーバへ送られる。内部ネットワークには、ファイアウォール等の外部からの不正アクセスを防止する手段が設けてあり、アクセスが制御されている。内部管理サーバへ送られた暗号済みの要求は内部暗号化モジュールで復号される。そして、ユーザ認証モジュールにより、ユーザ認証が行われる。アクセス制御モジュールは、ユーザ毎のアクセスルールが記述してあるアクセス制御リストを参照して今回のクライアントからのサービス要求に対し、アクセスを認めるか否かを判断するアクセス制御を行う。

【００３６】WWWサーバはアクセスが認められ、送られてきたサービス要求に対するサービス応答を提供する。暗号化して情報を送信するため、情報発信・共有サービス要求又は応答の内容が第三者へ漏洩することが防止でき、さらにユーザ認証を行うことで、本人からのサービス要求であることが確認でき、さらにアクセス制御をすることでアクセス制御リストに応じた情報発信・共有サービスの提供ができる。また、WWWサーバまたはクライアントの種類に限定されることなく、サービスの提供ができ、サービス提供のためにWWWサーバ及びクライアントへ特別にモジュール等を追加することなくサービスを利用することができる。

【００３７】また、この発明における安全な情報発信・共有システムをＨＴＴＰ上で実現することによりファイアウォール等に新たに特別な設定をすることなく、利用することができる。

【００３８】また、この発明における安全な情報発信・共有システムは、ユーザ認証に従来のユーザ名とパスワードの組み合わせでなく、公開鍵と秘密鍵の組み合わせによる電子証明書を用いることで、ネットワーク上での他人によるなりすましによる事故を防ぐことができる。

【００３９】また、この発明における安全な情報発信・共有システムは、内部管理サーバ又は外部管理サーバにキャッシュ制御手段を有するため、常にWWWサーバを介してサービス応答を引き出さなくても、各制御サーバのキャッシュからサービス応答を引き出すことができるため、通信トラフィックを減少させることができ、クライアントからのサービス要求に対する応答性能を向上させることができる。

【００４０】また、この発明における安全な情報発信・共有システムは、外部管理サーバ上のクライアント側キャッシュ消去手段により、クライアントのキャッシュ情報を消去することができるため、クライアント上のキャッシュに残った情報が同一のクライアントを利用する第三者に漏れることを防止することができる。

【００４１】また、この発明における安全な情報発信・共有システムは、WWWサーバと内部管理サーバ間の通信データも暗号化することで、WWWサーバと内部管理サーバ間の内部ネットワーク上の通信データについても第三者の盗聴、漏洩から保護することができる。

【００４２】また、この発明における安全な情報発信・共有システムは、クライアントと外部管理サーバ間の通信データも暗号化することで、クライアントと外部管理サーバ間の外部ネットワーク上の通信データについても第三者の盗聴、漏洩から保護することができる。尚、このクライアントと外部管理サーバ間のデータの暗号化は、インストール負担を考慮すると、暗号化ハブ等のハードウエアによる暗号化装置であることが望ましい。

【００４３】また、この発明における安全な情報発信・共有システムは、通信データを暗号化する一時暗号鍵を交換する期間を変更する一時暗号鍵交換手段を用いて、性能が低い制御サーバでも一定の応答性能を確保することが可能である。

【００４４】

【発明の実施の形態】実施の形態１．図２に本発明の実施の形態１に係る安全な情報発信・共有サービスシステムの構成を示す。情報発信・共有サービスを要求するクライアント２が、外部管理サーバ６を介して、通信ネットワーク３と接続され、この通信ネットワーク３が、ファイアウォール４を介して、内部ネットワークと接続されている。内部ネットワーク上には、WWWサーバ１と、内部管理サーバ５を有する。WWWサーバ１は従来と同じであり、内部管理サーバ５は、従来のアクセス制御サーバ８５と実質同じ機能を持つ。内部管理サーバ５は、暗号処理を行う内部暗号化モジュール７と、ユーザ認証を行うユーザ認証モジュール８と、アクセス制御を行うアクセス制御モジュール９とで構成されている。本発明の特徴は、従来クライアント２に設けていた暗号モジュール８６とアクセス制御サーバリスト８９を外部管理サーバ６に設けた点にある。これによりクライアント２毎に暗号モジュールとアクセス制御サーバリストのインストールが不要となり、特に外部管理サーバ６により管理されるクライアント２が多い程、そのメリットが大きい。図２に示すように外部管理サーバ６は複数のクライアント２によって形成される外部ローカルネットワークと情報ネットワークの接点に設けられる。外部ローカルネットワークは、社内ネットワーク等のような共通の管理者によって通信が管理されるネットワークである。

【００４５】また、クライアント２、外部管理サーバ６、WWWサーバ１、内部管理サーバ５はそれぞれネットワーク暗号化装置１２、１５、３２、３７を有する。ネットワーク暗号化装置１２、１５、３２、３７は、従来の暗号化モジュール８６のようなソフトウエアでなく、ハードウエアによる暗号化装置である。

【００４６】図３に公開鍵暗号方式による暗号化手段を設けたクライアント２と外部管理サーバ６の処理の概要を示す。クライアント２は、情報発信・共有サービス要求手段１１、クライアント側ネットワーク暗号化装置１

2及びクライアント側キャッシュ13で構成されている。

【0047】情報発信・共有サービス要求手段11によって情報発信・共有サービス要求14が作成される。クライアント側ネットワーク暗号化装置12はクライアント2と外部管理サーバ6間における情報の暗号/復号化を行う。この暗号化装置12は、ハードウエアの暗号化装置であり、従来のソフトウエアの暗号化装置と異なり、インストール不要なものである。クライアント側キャッシュ13はクライアント2に送られた情報を一時的に記憶するメモリ又はハードディスクである。

【0048】外部管理サーバ6は、外部管理サーバ側ネットワーク暗号化装置15、外部管理サーバ側暗号化モジュール16、クライアントリスト17、鍵取出し手段18、内部管理サーバリスト19、宛先変更手段20、外部管理サーバ側キャッシュ21、外部管理サーバ側キャッシュ制御手段22およびクライアント側キャッシュ消去手段23で構成される。

【0049】外部管理サーバ側ネットワーク暗号化装置15は、クライアント2と外部管理サーバ6間における情報の暗号/復号化する部分である。これも暗号化装置12と同じくハードウエアの暗号化装置である。外部管理サーバ側暗号化モジュール16は、情報発信・共有サービス要求14を暗号化し、キャッシュ禁止・暗号済み情報発信・共有サービス応答42を復号する。図2の外部暗号化モジュールと同じものである。クライアントリスト17は、外部管理サーバ6によって管理されている複数のクライアント2の情報（公開鍵、秘密鍵等）を格納する。鍵取出し手段18は、クライアントリスト17又は内部管理サーバリスト19からクライアント用公開鍵24、クライアント用秘密鍵25及び内部管理サーバ用公開鍵26を取り出す部分である。内部管理サーバリスト19は、内部管理サーバ5の情報（内部管理サーバ5のアドレス、内部管理サーバ用公開鍵26、内部管理サーバ5が管理するWWWサーバ1に関する情報等）を格納した部分である。宛先変更手段20はサービス要求の宛先をWWWサーバ1から内部管理サーバ5に変更する。外部管理サーバ側キャッシュ21は、内部管理サーバ5から送られた情報を一時的に記憶する部分である。外部管理サーバ側キャッシュ制御手段22は、外部管理サーバ側キャッシュ21を制御する部分である。クライアント側キャッシュ消去手段23はクライアント2に設けられたクライアント側キャッシュ13の記憶を消去する部分である。

【0050】クライアント2および外部管理サーバ6におけるサービス要求の動作について説明する。クライアント2は情報発信・共有サービス要求手段11により情報発信・共有サービス要求14を作成する。情報発信・共有サービス要求14はクライアント側ネットワーク暗号化装置12によって暗号化され、外部管理サーバ6へ送られる。外部管理サーバ6に送られた暗号化済みの情報発信・共有サービス要求14は外部管理サーバ側ネットワーク暗号化装置15によって復号される。続いて、電子署名、暗号化、宛先変更が外部管理サーバ6内で行われる。

【0051】電子署名の作成はハッシュ関数と、鍵取出し手段18によってクライアントリスト17から取り出されたクライアント用秘密鍵25を用いて行われる。内部管理サーバ5における電子署名の検証は、クライアント用公開鍵24を用いて行われるため、クライアント用公開鍵24が鍵取出し手段18によってクライアントリスト17から取り出され、HTTPのデータストリームに載せられる。サービス要求の暗号化は、予め内部管理サーバリスト内に保管された内部管理サーバ用公開鍵26によって行われる。内部管理サーバ用公開鍵26は、内部管理サーバリストから、鍵取出し手段18によって、取り出される。公開鍵暗号方式の暗号化では、公開鍵で暗号化した情報は、非対称な秘密鍵でなければ復号できない。したがって、暗号化されたサービス要求の内容は、内部管理サーバ5の有する内部管理サーバ用秘密鍵39でなければ復号できないため、通信ネットワーク3の途中で情報が第三者に盗難された場合であっても情報が解読されずにすむ。暗号化された電子署名、暗号化されたサービス要求及びクライアント用公開鍵24によってHTTPのデータストリームが形成される。続いてサービス要求の宛先が宛先変更手段20によってWWWサーバ1から内部管理サーバ5へ変更される。宛先変更には内部管理サーバリスト19内の宛先情報が参照される。

【0052】宛先変更済み暗号済み情報発信・共有サービス要求27が通信ネットワーク3を介して、内部管理サーバ5へ送られる。

【0053】図4に公開鍵暗号方式による暗号化手段を設けた内部管理サーバ5とWWWサーバ1の処理の概要を示す。

【0054】内部管理サーバ5は、内部管理サーバ側暗号化モジュール28、宛先変更手段29、アクセス制御リスト30、アクセス制御手段31、内部管理サーバ側ネットワーク暗号化装置32、鍵取出し手段33、キャッシュ禁止手段34、内部管理サーバ側キャッシュ35及び内部管理サーバ側キャッシュ制御手段36で構成されている。

【0055】内部管理サーバ側暗号化モジュール28は、宛先変更済み暗号済み情報発信・共有サービス要求27の復号、情報発信・共有サービス応答41の暗号化及び宛先変更済み暗号済み情報発信・共有サービス要求27のユーザ認証を行う部分である。図2の内部暗号化モジュールとユーザ認証モジュールの両方の機能を有する。宛先変更手段29は宛先を内部管理サーバ5からWWWサーバ1に変更する部分である。アクセス制御リス

ト３０は各ユーザのアクセス許可条件を格納した部分である。アクセス制御手段３１はアクセス制御リスト３０を参照してアクセスの可否を判定する部分である。内部管理サーバ側ネットワーク暗号化装置３２は内部管理サーバ５とWWWサーバ１間における情報の暗号／復号化を行う部分である。鍵取出し手段３３は、内部管理サーバ５内の内部管理サーバ用秘密鍵３９を取り出す部分である。キャッシュ禁止手段３４は通信ネットワーク３上に存在する各サーバ上のキャッシュに暗号化された暗号済み情報発信・共有サービス応答４１を残さない旨の指令を追加する部分である。内部管理サーバ側キャッシュ３５は内部管理サーバ５のキャッシュである。内部管理サーバ側キャッシュ制御手段３６は内部管理サーバ側キャッシュ３５を制御する部分である。

【００５６】WWWサーバ１は、WWWサーバ側ネットワーク暗号化装置３７及び情報発信・共有サービス提供手段３８で構成される。WWWサーバ側ネットワーク暗号化装置３７は内部管理サーバ５とWWWサーバ１間における情報の暗号／復号化を行う部分であり、情報発信・共有サービス提供手段３８は、情報発信・共有サービス応答４１を提供する部分である。

【００５７】次に内部管理サーバ５でのサービス要求動作を説明する。外部管理サーバ６から通信ネットワーク３及びファイアウォール４を介して宛先変更済み暗号済み情報発信・共有サービス要求２７が送られて来る。内部管理サーバ５では、ユーザ認証、要求の復号化、宛先変更、アクセス制御が行われる。

【００５８】ユーザー認証は、内部管理サーバ側暗号化モジュール２８により一緒に送られてきたクライアント用公開鍵２４を用いて行われる。クライアント用秘密鍵２５で暗号化した電子署名を、送られてきたクライアント用公開鍵２４を用いて復号を試み、復号できれば、クライアント用秘密鍵２５を有するユーザーであると認証する。暗号化されたサービス要求の復号は、鍵取出し手段３３により取り出された内部管理サーバ用秘密鍵３９を用いて行われる。続いて宛先変更手段２９により、宛先変更済み暗号済み情報発信・共有サービス要求２７の宛先が内部管理サーバ５からWWWサーバ１に戻される。

【００５９】アクセス制御はアクセス制御手段３１によりアクセス制御リスト３０を参照して行われる。アクセス制御リスト３０には、ユーザ毎のアクセスの設定条件が備えられており、その条件に基づいて、今回宛先変更済み暗号済み情報発信・共有サービス要求２７を出したユーザーに対してアクセスを許可するかどうかの判定を行う。

【００６０】アクセスが許可されなかった場合は、WWWサーバ１へのサービス要求は許可しない旨のエラーメッセージが外部管理サーバ６経由でクライアント２に送られ、サービス要求手続きは完了する。アクセスが許可された場合は、情報発信・共有サービス要求が内部管理サーバ側ネットワーク暗号化装置３２で暗号化されWWWサーバ１に送られる。ここでも、内部管理サーバ５とWWWサーバ１間が平文でなく暗号文で送られるため、情報の安全が確保される。

【００６１】WWWサーバ１では、送られて来たサービス要求をWWWサーバ側ネットワーク暗号化装置３７で復号する。こうして最終的に平文の情報発信・共有サービス要求４０が情報発信・共有サービス提供手段３８に届けられる。

【００６２】続いて、WWWサーバ１及び内部管理サーバ５でのサービス応答動作について説明する。図４のWWWサーバ１の情報発信・共有サービス提供手段３８において、届けられた情報発信・共有サービス要求４０に対する情報発信・共有サービス応答４１が作成される。このサービス応答４１はWWWサーバ側ネットワーク暗号化装置３７によって暗号化され内部管理サーバ５へ送られる。

【００６３】内部管理サーバ側ネットワーク暗号化装置３２によって、送られて来た暗号化済みの情報発信・共有サービス応答４１を復号する。内部管理サーバ５において、サービス応答４１の暗号化と電子署名、キャッシュ禁止指令の付加が行われる。

【００６４】サービス応答４１の暗号化は、内部管理サーバ側暗号化モジュール２８によってクライアント用公開鍵２４を用いて行われる。電子署名は、内部管理サーバ用秘密鍵３９が用いられる。暗号化済みサービス応答は、続いて、キャッシュ禁止手段３４によりキャッシュ禁止指令が付加される。キャッシュ禁止指令とは、外部管理サーバ６と内部管理サーバを除く通信ネットワーク３上の各サーバのキャッシュにキャッシュ禁止・暗号済み情報発信・共有サービス応答４２を残さない旨の指令である。係るキャッシュ禁止指令を追加したキャッシュ禁止暗号済み情報発信・共有サービス応答４２が通信ネットワーク３を介して外部管理サーバ６へ送られる。キャッシュ禁止指令が追加された応答情報であるため、他のサーバ上にキャッシュが残らないため、通信ネットワーク３上に存在する各サーバのキャッシュからの第三者の改ざん、盗聴を防ぐことができる。

【００６５】続いて、外部管理サーバ６及びクライアント２でのサービス応答動作について図３で説明する。外部管理サーバ６に内部管理サーバ５からキャッシュ禁止・暗号済み情報発信・共有サービス応答４２が送られてくる。外部管理サーバ側暗号化モジュール１６では、サービス応答の復号を行う。復号はクライアントリスト１７内のクライアント用秘密鍵２５によって行われる。こうして、復号されたサービス応答は、外部管理サーバ側ネットワーク暗号化装置により、暗号化され、クライアント２に送られる。クライアント２では、クライアント側ネットワーク暗号化装置１２で復号しサービス応答４

3を平文として取り出す。このようにして、クライアント2は、情報発信・共有サービス応答43を受けることができる。

【0066】尚、クライアント2がWWWサーバ1へ向けて同じサービス要求をしており、かつ外部管理サーバ側キャッシュ21に有効なサービス応答が残っている場合は、外部管理サーバ側キャッシュ制御手段23がそのサービス応答を取り出して、クライアント2へ送る。これにより、クライアント2は、以前と同じサービス要求であれば、WWWサーバ1と通信することなく、外部制御サーバ6からサービス応答が入手でき、その結果、WWWサーバ1との応答回数を減らすことができ、システム全体の応答性能が向上する。

【0067】この場合、外部管理サーバ6は、クライアント2とその利用者を、最初のアクセス時にユーザ名とパスワード入力等をさせる等の認識方法をとることにより、ユーザ認証を行い、各利用者ごとに、キャッシュを管理する。

【0068】また、クライアント2がWWWサーバ1へ向けて同じサービス要求をしており、内部管理サーバ側キャッシュ35に有効なサービス応答が残った場合は、同様に、内部管理サーバ側キャッシュ制御手段36によって取り出され、クライアント2へ送られる。このため、内部管理サーバ5とWWWサーバ1間の応答回数を減らすことができ、システム全体の応答性能が向上することになる。

【0069】さらに、外部管理サーバ6は、クライアント側キャッシュ消去手段23を有し、外部管理サーバ6から、クライアント側キャッシュ13を制御できる。クライアント2が初めて外部管理サーバ6にアクセスしたときにクライアント2にクライアント側キャッシュ消去手段23が自動的にロードされる。このキャッシュ消去手段23は、クライアント2で起動したWebブラウザが終了した時点で、キャッシュが格納されているディレクトリ下のファイルを削除するプログラムを実行する。従って、同一クライアント2を複数の利用者が使用する場合でも、利用者の使用終了毎にキャッシュに残った情報が消去されるため、他の利用者へ情報が漏洩することを防ぐことができる。

【0070】実施の形態2

図5、6で公開鍵暗号方式と対称鍵暗号方式を組み合わせた暗号化方式による外部管理サーバ6及び内部管理サーバ5での暗号化処理の概要を説明する。各サーバの構成は、図3、4とほぼ同じである。ネットワーク暗号化装置等は省略して説明する。

【0071】平文の状態の情報発信・共有サービス要求が、クライアント2から送られてくる。鍵取出し手段18によってクライアントリスト17からクライアント用公開鍵24とクライアント用秘密鍵25が取り出される。また、鍵取出し手段18によって内部管理サーバリスト19から内部管理サーバ用公開鍵26が取り出される。さらに一時暗号鍵生成手段70によって一時暗号鍵71が生成される。

【0072】外部管理サーバ側暗号化モジュール16はクライアント用秘密鍵25を用いて電子署名を行い、一時暗号鍵71を用いて情報発信・共有サービス要求14を暗号化し、さらに内部管理サーバ用公開鍵26を用いて一時暗号鍵71を暗号化する。一時暗号鍵とクライアント用公開鍵は、サービス要求と一緒に内部管理サーバ5へ送られる。

【0073】図6において、暗号化されたサービス要求が、外部管理サーバ6から送られると、内部管理サーバ5は、鍵取出し手段33により、内部管理サーバ用秘密鍵39を取り出す。内部管理サーバ用秘密鍵39を用いて内部管理サーバ用公開鍵で暗号化した一時暗号鍵72を復号して取り出す。この取り出した一時暗号鍵72を用いてサービス要求を復号する。さらに送られたクライアント用公開鍵24を用いて電子署名の検証を行うことでユーザ認証を行う。平文となったサービス要求はWWWサーバ1に送られる。

【0074】WWWサーバ1からの平文のサービス応答が、内部管理サーバ5に送られると、内部管理サーバ側暗号化モジュール28が一時暗号鍵72を用いてサービス応答を暗号化し、外部管理サーバ6へ送る。図5において、暗号化されたサービス応答が外部管理サーバ6へ送られると、外部管理サーバ側暗号化モジュール16が一時暗号鍵71を用いてサービス応答を復号する。平文となったサービス応答がクライアント2へ送られる。

尚、この実施の形態においては、一時暗号鍵はサービス要求毎に作成される。

【0075】実施の形態3

本実施の形態は、一時暗号鍵71、72の交換時期を変動させたものである。図7に一時暗号鍵交換手順のフローチャートを示す。クライアント2からのサービス要求がくると、最初のサービス要求かどうか外部管理サーバ6にて判断される（S101）。最初のサービス要求であれば、一時暗号鍵71、72の交換がされる（S103）。一時暗号鍵71、72の交換は外部管理サーバ6と内部管理サーバ5の間で行われる。一時暗号鍵71、72の交換は、外部管理サーバ6にて新たに一時暗号鍵が作成され、内部管理サーバ5へ新しい鍵を送ることにより行われる。この一時暗号鍵71、72の送信は電子証明書を用いた公開鍵暗号方式が用いられる。鍵交換が成功すれば（S104）、外部管理サーバ6と内部管理サーバ5間でその鍵を用いて暗号化及び復号の暗号化処理が行われる（S105）。

【0076】S101で最初のサービス要求ではない場合、外部管理サーバ6は続いてサービス要求先は前回の要求と同じかどうか判断する（S102）。同じであれば、一時暗号鍵71、72は交換されずに暗号化処理が

行われる（Ｓ１０５）。サービス要求先が前回の要求と異なれば、一時暗号鍵７１、７２の交換を行う（Ｓ１０３）。Ｓ１０２でサービス要求先が同じかどうか判断することで、一時暗号鍵７１、７２の交換間隔を動的に変更することができる。このＳ１０２の判断内容は、任意に選択することができる。例えば、ある一定時間経過後に一時暗号鍵を交換したり、ある一定回数サービス要求をした時に一時暗号鍵を交換するようにすることができる。サービス要求毎に一時暗号鍵の交換をすれば、安全面では優れるが、公開鍵暗号方式による鍵の交換に時間がかかり、応答速度が遅いという欠点があるが、この一時暗号鍵の交換間隔を動的に変更することによって、応答速度を高めることができる。したがって、使用される様々な性能のサーバのうち、性能の劣るサーバであっても一定の応答性能を確保することができる。

【００７７】実施の形態４

図８は本発明でのＨＴＴＰデータストリームの概要図である。ＨＴＴＰデータストリームは、指令、ヘッダ群、区切り子及び本体からなる。指令には、データストリームの宛先が格納される。ヘッダには、本体の長さ、キャッシュ禁止情報等が追加され格納される。本体には、暗号化されたデータが格納される。

【００７８】外部管理サーバ６から内部管理サーバ５へ出力されるデータストリームは以下のようになる。指令部分は宛先変更手段によって宛先がＷＷＷサーバ１から内部管理サーバ５へ変更される。ヘッダ３では、データストリームが本発明のシステムによって生成されたものであることを示す情報及び一時暗号鍵７１、７２の状態（要交換、交換済み、交換の成否）を示す情報が追加される。本体部分では、元の宛先及び情報発信・共有サービス要求、ユーザ認証に用いる元の宛先に対する電子署名、クライアント２の公開鍵、一時暗号鍵等が暗号化されて格納される。

【００７９】内部管理サーバ５から外部管理サーバ６へ出力されるデータストリームは、以下のようになる。指令部分にはＷＷＷサーバ１からサービス要求に対する状態が格納される。ヘッダ２には通信ネットワーク３上に存在する各サーバ（内部管理サーバ５及び外部管理サーバ６を除く）上のキャッシュに情報発信・共有サービス応答が残らない旨の指令が追加される。ヘッダ３にはデータストリームが本発明のシステムによって生成されたものであることを示す情報及び一時暗号鍵の状態を示す情報が追加される。本体部分では、情報発信・共有サービス応答、一時暗号鍵等が暗号化されて格納される。このように、情報発信・共有サービスをＨＴＴＰ上で実現したので、ファイアウォール４等に新たな設定を必要としない。

【００８０】

【発明の効果】以上のように、この発明における安全な情報発信・共有サービス方法は、クライアントの情報発信・共有サービス要求手段１１により情報発信・共有サービスを要求し、この要求を外部管理サーバ６の外部管理サーバ側暗号化モジュールにより暗号化し、内部管理サーバ５で送られてきた宛先変更済み暗号済み要求を内部管理サーバ側暗号化手段で復号しアクセス制御リストを参照してアクセス制御を行い、ＷＷＷサーバ１で送られてきた要求に対する応答を提供し、内部管理サーバで提供された応答を内部管理サーバ側暗号化手段で暗号化し、外部管理サーバ６で送られてきたキャッシュ禁止・暗号済み応答を復号するようにしたので、情報発信・共有サービス要求又は応答の内容が通信ネットワークにおいて第三者に漏れることを防ぐことが可能であり、アクセス制御リストに応じた情報発信・共有サービスの提供が可能であり、ＷＷＷサーバ１及びクライアント２の種類に依存せず、ＷＷＷサーバ１及びクライアント２への暗号化モジュールのインストール不要となり、さらに新たに強固な暗号方式が開発された場合に、内部管理サーバと外部管理サーバのモジュールを入れ替えることで新たな暗号方式にすぐに対応できるという効果がある。

【００８１】また、この発明における安全な情報発信・共有サービス方法は、情報発信・共有サービスをＨＴＴＰ上で実現したので、ファイアウォール４等に新たな設定を必要としないという効果がある。

【００８２】また、この発明における安全な情報発信・共有サービス方法は、ユーザ認証に従来のユーザ名とパスワードの組合わせの代わりに電子証明書（公開鍵と秘密鍵の組合せ）を用いることで、ネットワーク上での他人のなりすましを防ぐことができるという効果がある。

【００８３】また、この発明における安全な情報発信・共有サービス方法は、外部管理サーバ６と内部管理サーバ５とのキャッシュ制御手段により通信トラフィックの減少と応答性能の向上が実現できるという効果がある。

【００８４】また、この発明における安全な情報発信・共有サービス方法は、外部管理サーバ６のクライアント側キャッシュ消去手段によりクライアント上のキャッシュを制御するので、クライアントのキャッシュから情報が同じクライアントを使用する第三者に漏れることを防ぐことができるという効果がある。

【００８５】また、この発明における安全な情報発信・共有サービス方法は、ＷＷＷサーバ１と内部管理サーバ５との間の通信データをネットワーク暗号化装置によって暗号化するようにしたので、ＷＷＷサーバ１と内部管理サーバ５との間のデータを保護できるという効果がある。

【００８６】また、この発明における安全な情報発信・共有サービス方法は、クライアントと外部管理サーバ６との間の通信データをネットワーク暗号化装置によって暗号化するようにしたので、クライアントと外部管理サーバ６との間のデータを保護できるという効果がある。

【００８７】また、この発明における安全な情報発信・

共有サービス方法は、外部管理サーバ6にて外部管理サーバ6と内部管理サーバ5間の通信の際に用いる暗号鍵を変更する間隔を変更できるようにしたので、サーバの性能に応じて応答時間を可変にできるという効果がある。

【図面の簡単な説明】

【図1】 従来の情報発信・共有システムの構成図である。

【図2】 今回のこの発明における安全な情報発信・共有サービスシステムの構成図である。

【図3】 公開鍵暗号方式を利用したクライアント2及び外部管理サーバ6の処理の概要を示す図である。

【図4】 公開鍵暗号方式を利用した内部管理サーバ5及びWWWサーバ1の処理の概要を示す図である。

【図5】 公開鍵暗号方式及び対称鍵暗号方式を利用した外部管理サーバ6での暗号化処理の概要を示す図である。

【図6】 公開鍵暗号方式及び対称鍵暗号方式を利用した内部管理サーバ5での暗号化処理の概要を示す図である。

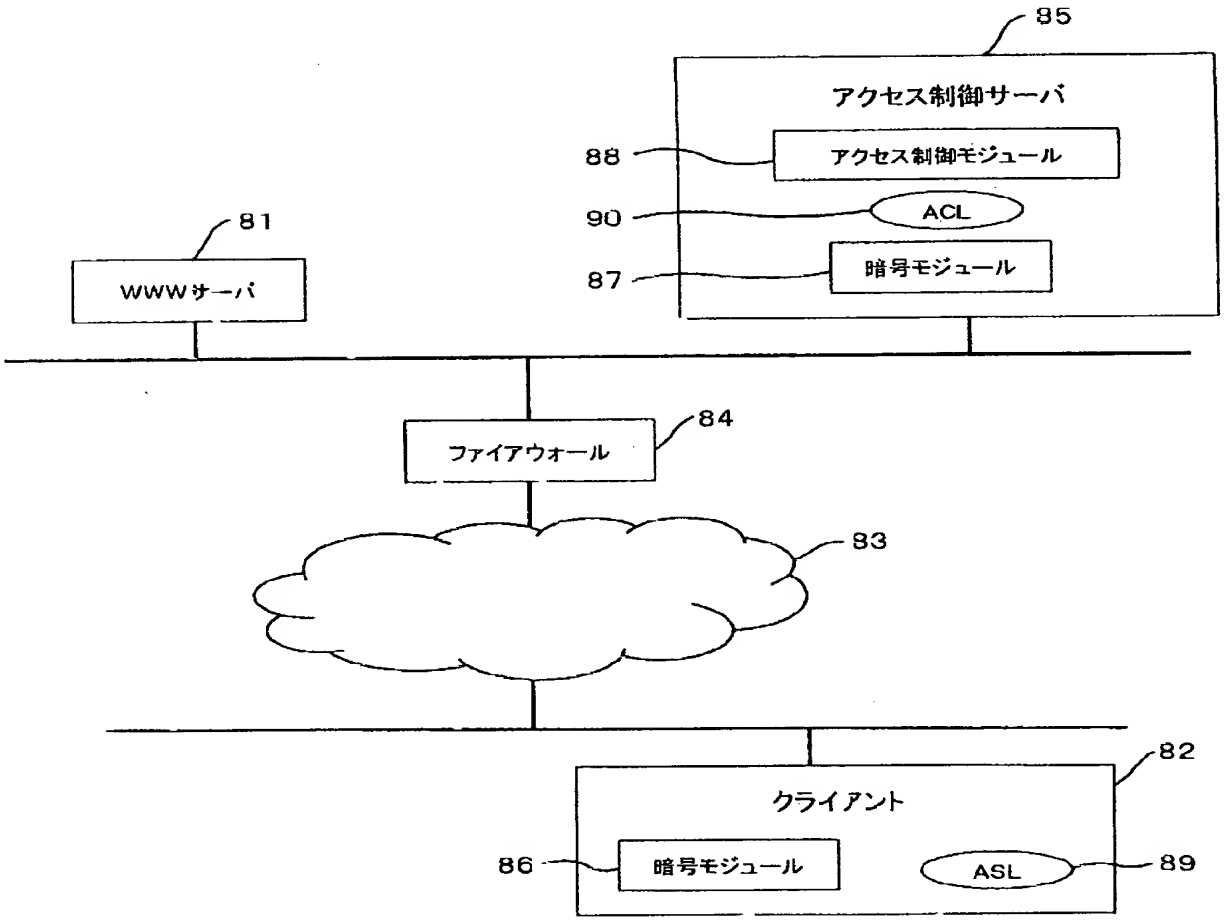
【図7】 一時暗号鍵の交換手順のフローチャートである。

【図8】 HTTPデータストリームを示す図である。

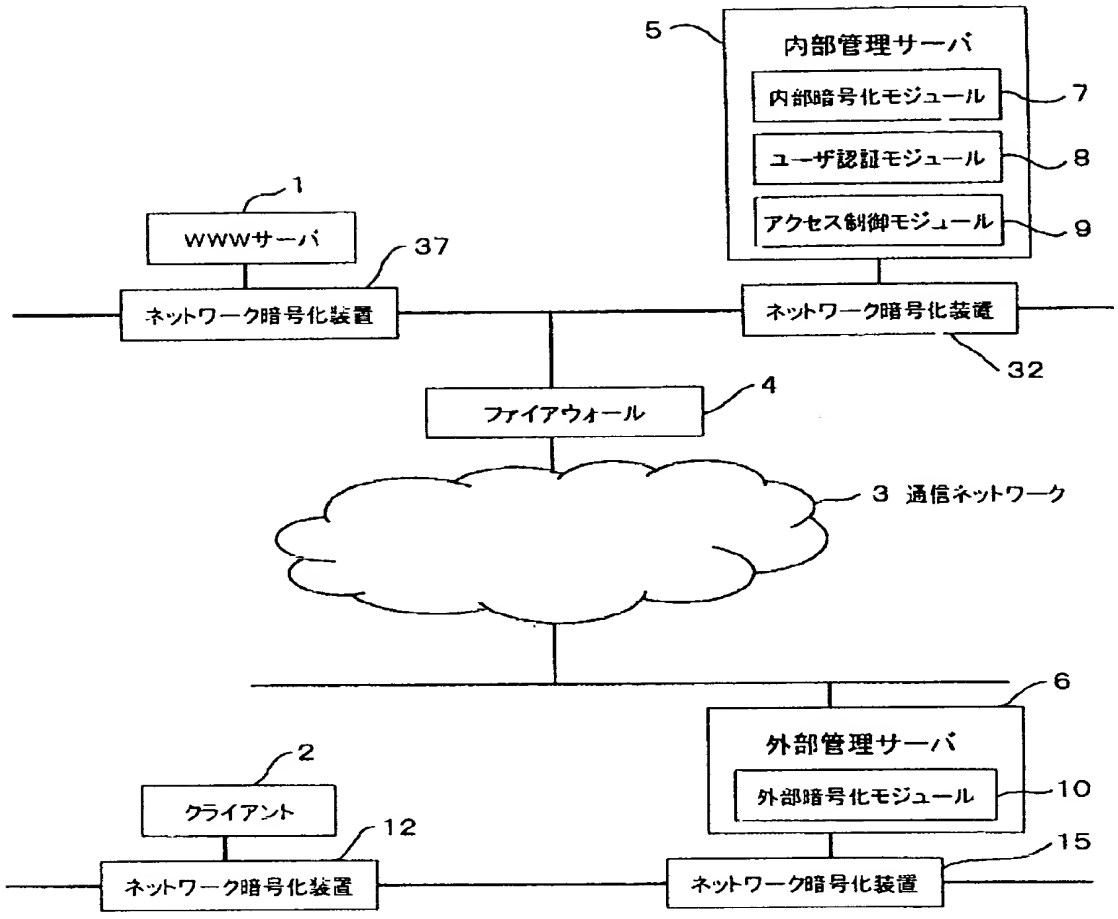
【符号の説明】

1，81 WWWサーバ、2，82 クライアント、3，83 通信ネットワーク、4，84 ファイアウォール、5 内部管理サーバ、6 外部管理サーバ、7 内部暗号化モジュール、8 ユーザ認証モジュール、9 アクセス制御モジュール、10 外部暗号化モジュール、11 情報発信・共有サービス要求手段、12 クライアント側ネットワーク暗号化装置、13 クライアント側キャッシュ、14 情報発信・共有サービス要求、15 外部管理サーバ側ネットワーク暗号化装置、16 外部管理サーバ側暗号化モジュール、17 クライアントリスト、18 鍵取出し手段、19 内部管理サーバリスト、20 宛先変更手段、21 外部管理サーバ側キャッシュ、22 外部管理サーバ側キャッシュ制御手段、23 クライアント側キャッシュ消去手段、24 クライアント用公開鍵、25 クライアント用秘密鍵、26 内部管理サーバ用公開鍵、27 宛先変更済み暗号済み情報発信・共有サービス要求、28 内部管理サーバ側暗号化モジュール、29 宛先変更手段、30 アクセス制御リスト、31 アクセス制御手段、32 内部管理サーバ側ネットワーク暗号化装置、33 鍵取出し手段、34 キャッシュ禁止手段、35 内部管理サーバ側キャッシュ、36内部管理サーバ側キャッシュ制御手段、37 WWWサーバ側ネットワーク暗号化装置、38 情報発信・共有サービス提供手段、39 内部管理サーバ用秘密鍵、40 情報発信・共有サービス要求、41，43 情報発信・共有サービス応答、42 キャッシュ禁止・暗号済み情報発信・共有サービス応答、70 一時暗号鍵生成手段、71，72 一時暗号鍵、85 アクセス制御サーバ、86クライアント側暗号モジュール、87 アクセス制御サーバ側暗号モジュール、88 アクセス制御モジュール、89 アクセス制御サーバリスト、90 アクセス制御リスト。

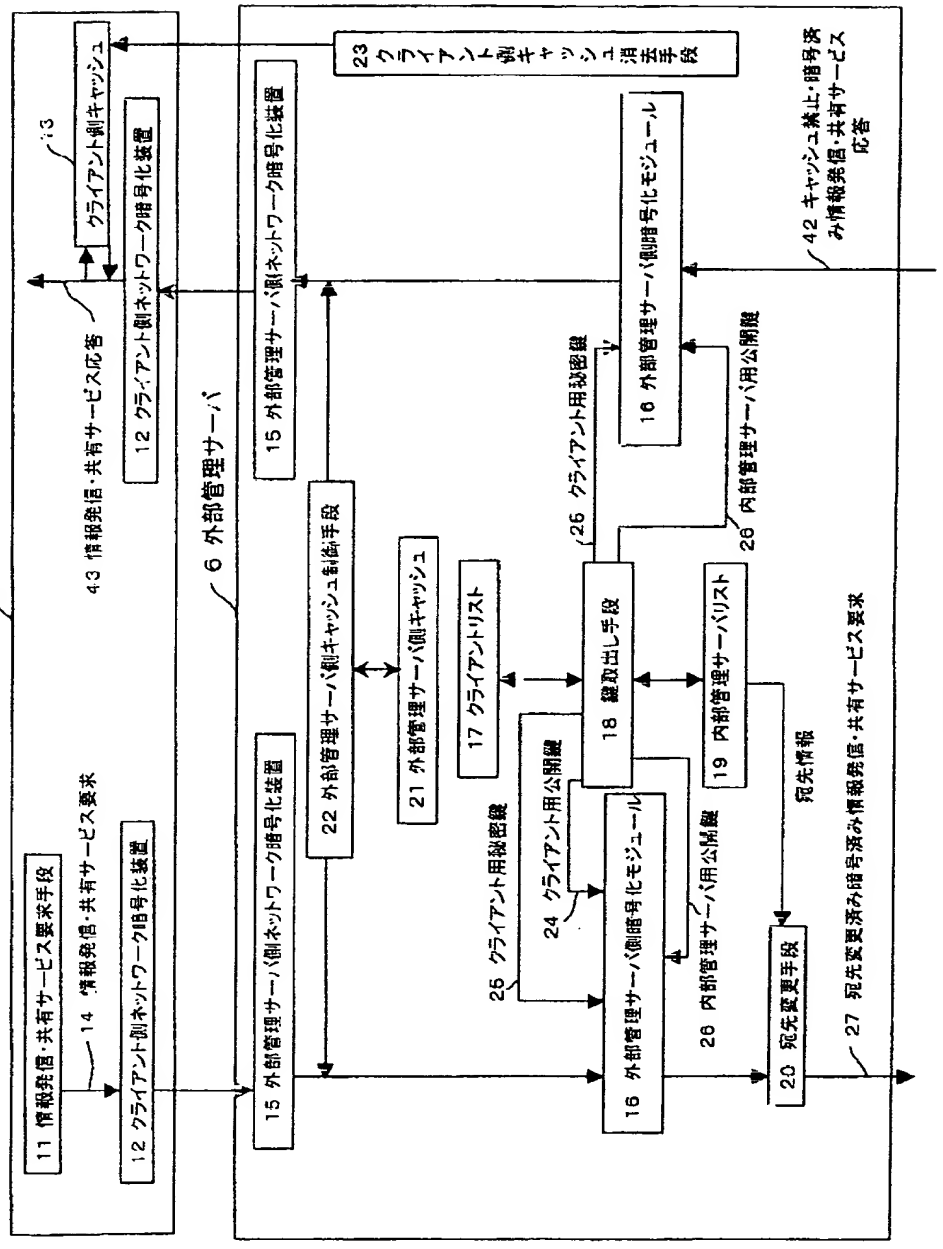
【図1】


85
アクセス制御サーバ
88
アクセス制御モジュール
90
ACL
87
暗号モジュール
81
WWWサーバ
84
ファイアウォール
83
82
クライアント
86
暗号モジュール
ASL
89

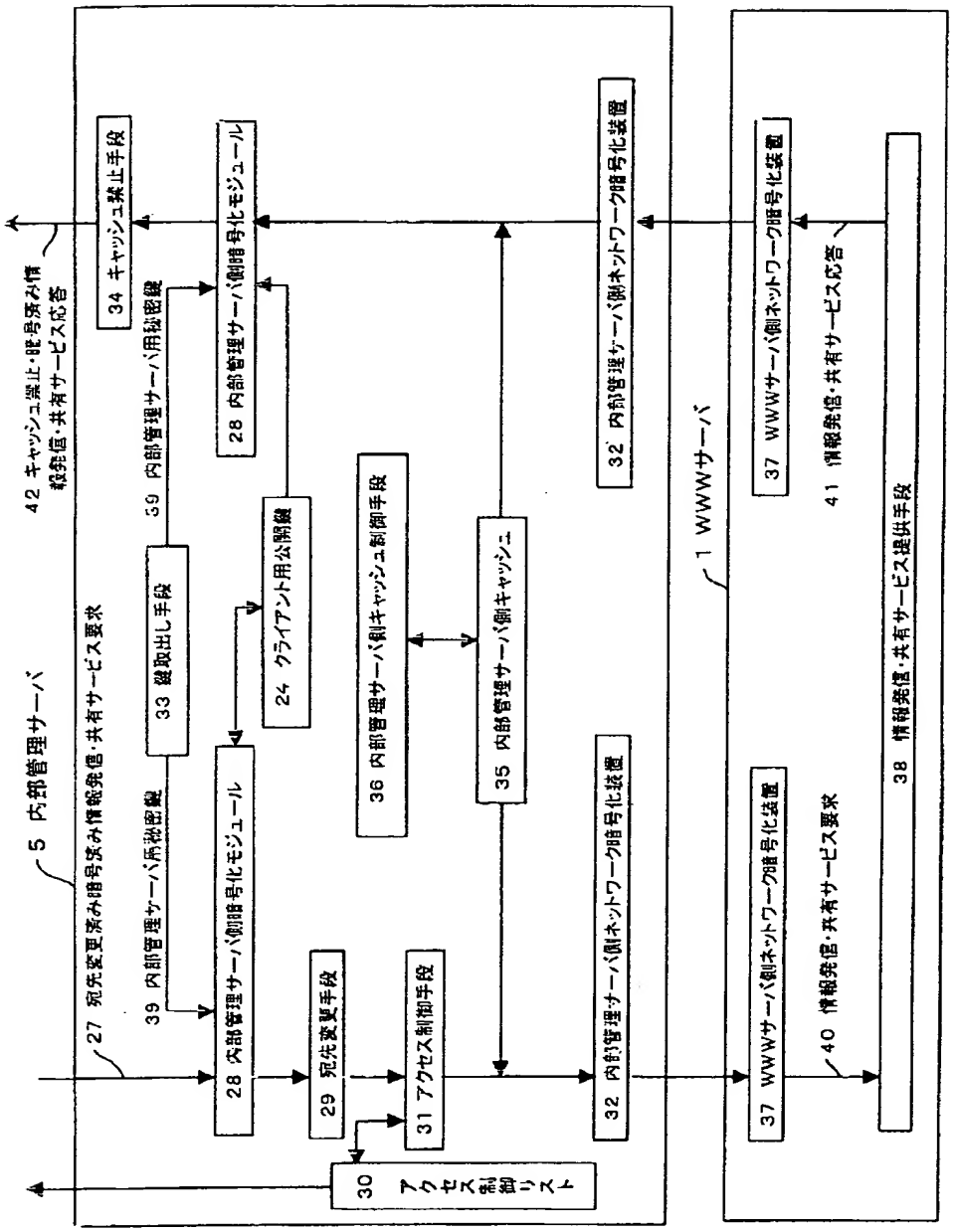
【図２】


5
内部管理サーバ
内部暗号化モジュール
7
ユーザ認証モジュール
8
アクセス制御モジュール
9
1
WWWサーバ
37
ネットワーク暗号化装置
ネットワーク暗号化装置
32
ファイアウォール
4
3 通信ネットワーク
6
外部管理サーバ
外部暗号化モジュール
10
2
クライアント
12
ネットワーク暗号化装置
15
ネットワーク暗号化装置

【図3】

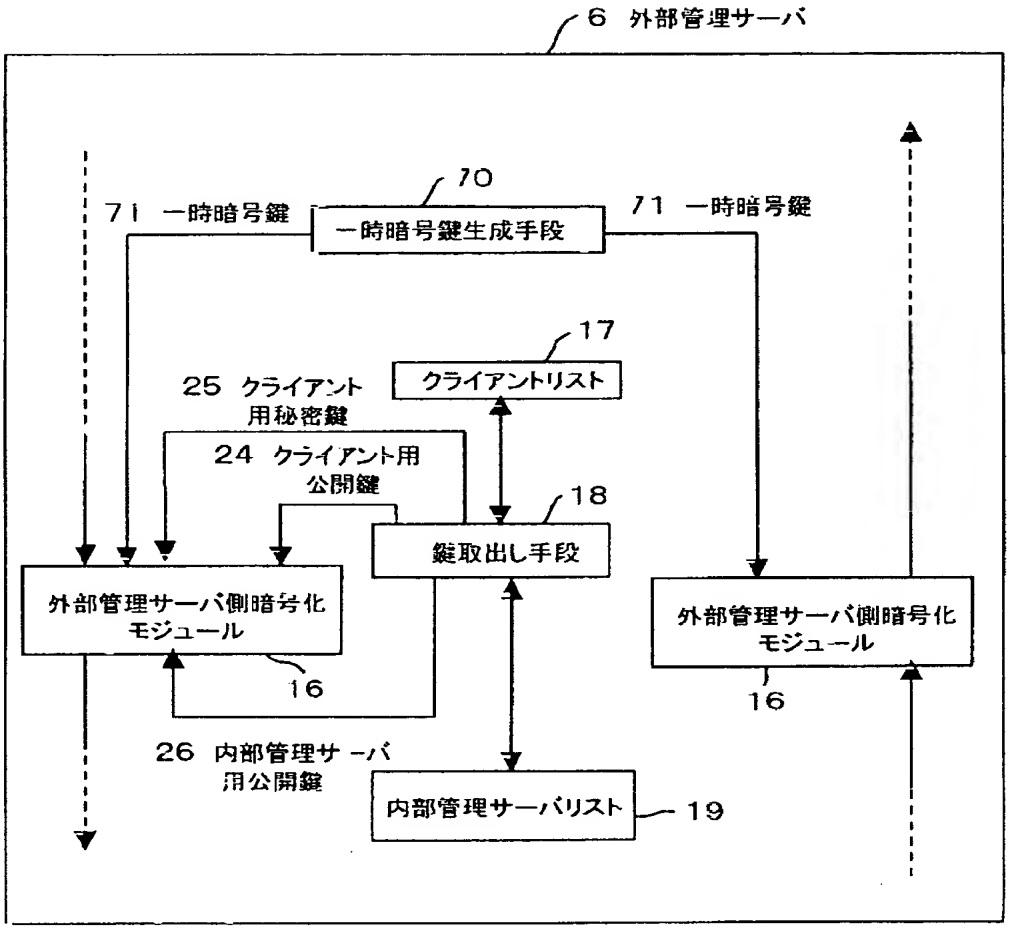

2 クライアント
11 情報発信・共有サービス要求手段
14 情報発信・共有サービス要求
12 クライアント側ネットワーク暗号化装置
43 情報発信・共有サービス応答
13 クライアント側キャッシュ
12 クライアント側ネットワーク暗号化装置
6 外部管理サーバ
15 外部管理サーバ側ネットワーク暗号化装置
15 外部管理サーバ側ネットワーク暗号化装置
22 外部管理サーバ側キャッシュ制御手段
21 外部管理サーバ側キャッシュ
17 クライアントリスト
26 クライアント用秘密鍵
24 クライアント用公開鍵
18 鍵取出し手段
16 外部管理サーバ側暗号化モジュール
19 内部管理サーバリスト
26 内部管理サーバ用公開鍵
20 宛先変更手段
宛先情報
27 宛先変更済み暗号済み情報発信・共有サービス要求
26 クライアント用秘密鍵
16 外部管理サーバ側暗号化モジュール
26 内部管理サーバ用公開鍵
23 クライアント側キャッシュ消去手段
42 キャッシュ禁止・暗号済み情報発信・共有サービス応答
外部管理サーバの処理の概要

【図4】



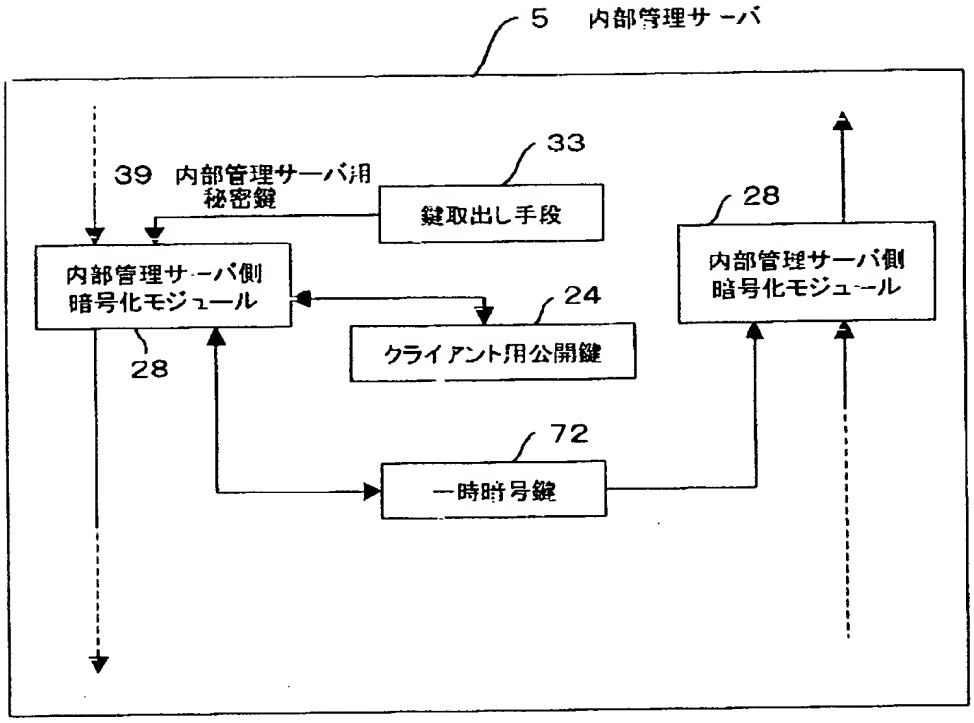
内部管理サーバの処理の概要

【図５】



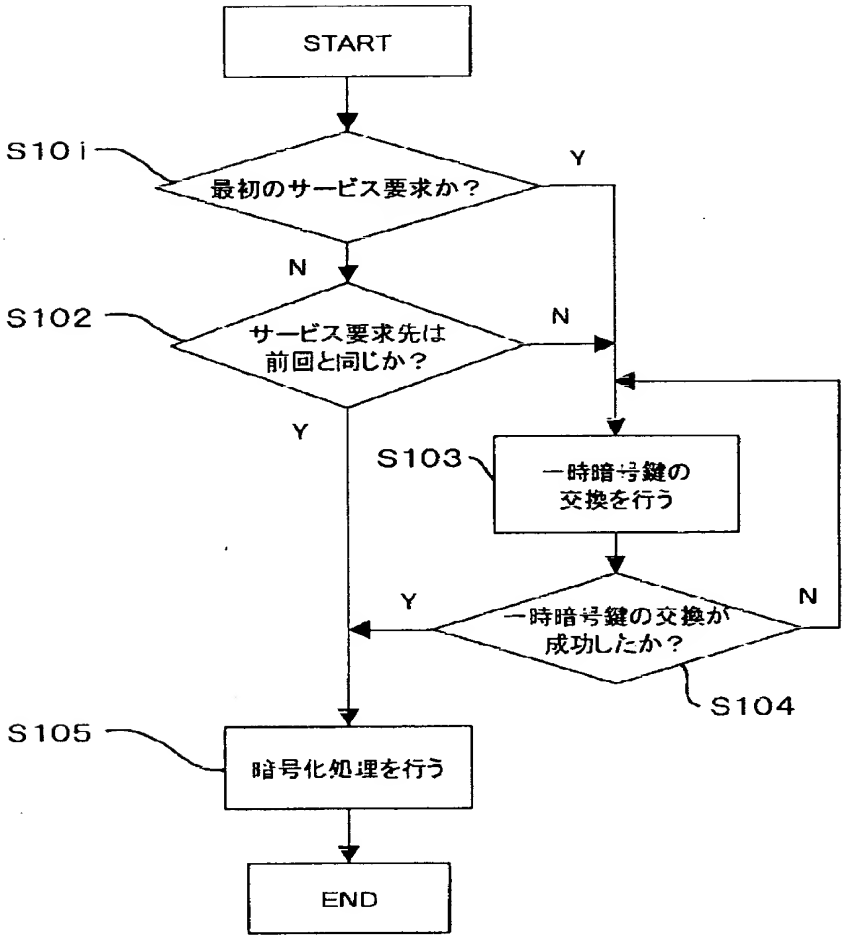
外部管理サーバでの暗号化処理の概要

【図６】



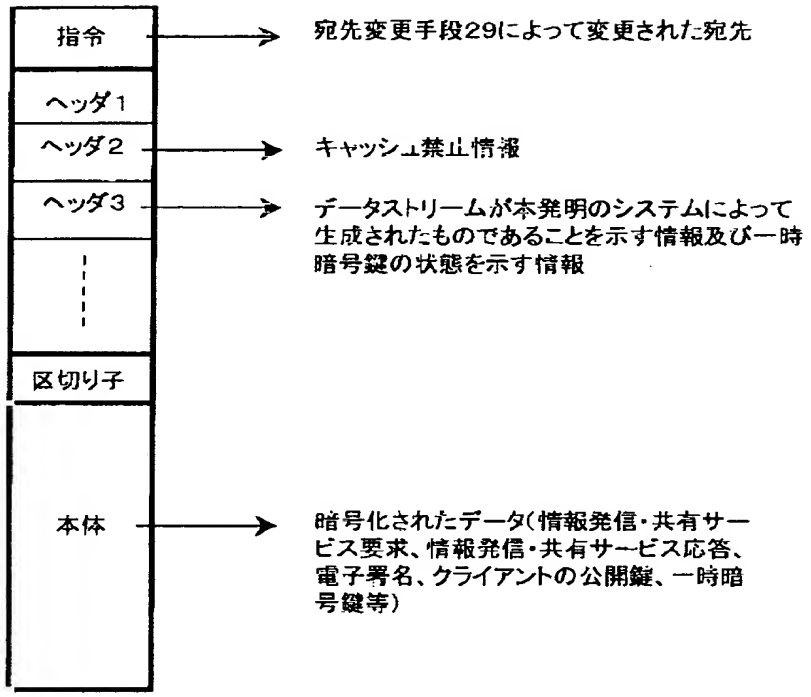
内部管理サーバでの暗号化処理の概要

【図7】



一時暗号鍵交換手順

【図８】



HTTPのデータストリームの概要